C. REMARKS

1. Summary of the Claims

Claims 1-20 were pending in the application prior to this amendment. Claims 1, 8, and 14 are independent claims. Claims 1, 3, 7, 8, 10, 13, 14, 16, and 20 have been amended. Claims 2, 4, 6, 9, 12, 15, 17, and 19 have been cancelled. Claims 21-26 have been added. No new matter has been added. Claims 1, 3, 5, 7, 8, 10, 11, 13, 14, 16, 18, and 20-26 are currently pending in the application. Reconsideration of the claims is respectfully requested.

2. Examiner Interview

Applicants note with appreciation the telephonic interview conducted between Applicants' representative and the Examiner on April 14, 2005. During the telephonic interview, the Examiner and Applicants' representative discussed the 103 references (Goldstone, U.S. Publication No. 2002/0101819, and Klaus, U.S. Patent No. 5,892,903). In particular, Applicants' representative informed the Examiner that Applicants are submitting a declaration, pursuant to 37 C.F.R. § 1.131, with this response, declaring that Applicants conceived of the claimed invention before the filing date of Goldstone and showed diligence from the date of conception to the filing date of the subject application. Applicants' representative suggested incorporating the limitations of original dependent claim 2, which was rejected using Goldstone, into independent claim 1 in order for claim 1 to read over the art of record.

In addition, Applicants' representative discussed the differences between Goldstone and the limitations included in

Applicants' claim 3, which are discussed in further detail below.

Applicants' representative also informed the Examiner that Applicants are adding new claims in this response, each of which are supported by the original specification. While no agreement was reached regarding the claims, Applicants respectfully submit that, as explained in further detail below, the amendments made to independent claims 1, 8, and 14, place these claims and their respective dependent claims in condition for allowance.

3. Drawings

Applicants note that the Examiner did not indicate whether the formal drawings, filed with Applicants' application, are accepted by the Examiner. Applicants respectfully requests that the Examiner indicate whether the formal drawings are accepted in the next office communication.

4. Claim Rejections

Claims 1, 8, and 14 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Gupta et al. (U.S. Patent No. 6,389,532, hereinafter "Gupta"). Applicants respectfully traverse these rejections.

Claims 3, 5, 10, 11, 16, and 18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Gupta in view of Goldstone (U.S. Publication No. 2002/0101819, hereinafter "Goldstone"). Applicants respectfully traverse these rejections.

The independent claims as amended are directed to "preventing malicious network attacks" with limitations comprising:

- receiving a packet from a client computer;
- identifying the client computer by a source IP address;
- calculating a number of packets received using the source IP address during a time interval;
- comparing the number of packets received with one or more configuration settings;
- determining an action from a plurality of actions based on the comparing; and
- executing the action.

Applicants have amended claim 1 to incorporate the limitations of original claim 4. In addition, as discussed with the Examiner, Applicants have amended claim 1 to incorporate the limitations of original claim 2, which was rejected using the Goldstone reference. Applicants respectfully assert that Applicants conceived of the claimed invention before the filing date of Goldstone, and showed diligence from the date of conception to the filing date of the subject application. A declaration, pursuant to 37 C.F.R. § 1.131, has been duly executed by Applicant Dwip Banerjee and is included with this Response. Mr. Banerjee declares that he conceived of, in the United States of America, the invention described and claimed in the subject application prior to January 31, 2001. Mr. Banerjee further showed diligence from the date of conception to the filing date of the subject application. Exhibit "A" to Mr. Banerjee's declaration is the IBM Invention Disclosure Form that disclosed Applicants'

claimed invention. This disclosure was submitted to the IBM Intellectual Property Law Department in Austin, Texas prior to January 31, 2001. Mr. Banerjee's declaration under 37 C.F.R. § 1.131, therefore, removes the Goldstone reference from consideration as prior art. Because, for the aforesaid reasons, the Goldstone reference is not prior art with respect to Applicants' claimed invention, Applicants respectfully assert that since claim 1 as amended includes the limitations of original claim 2 that was rejected using Goldstone, that amended claim 1 is allowable over the art of record.

Claim 8 as amended is an information handling system claim including the same limitations of amended claim 1 and, therefore, is allowable for the same reason as amended claim 1. Claim 14 as amended is a computer program product claim including the same limitations of amended claim 1 and, therefore, is allowable for the same reason as amended claim 1.

Notwithstanding the fact that claims 3, 5, 10, 11, 16, and 18 are each dependent upon one of the amended claims 1, 8, or 14, and therefore allowable for the same reasons as their independent claims, claims 3, 5, 10, 11, 16, and 18 were rejected using the Goldstone reference, which is removed as discussed above. Therefore, claims 3, 5, 10, 11, 16, and 18 are allowable over the art of record.

In addition, notwithstanding the fact that claim 3 is allowable for the reasons discussed above, claim 3 adds the limitations to amended claim 1 of:

- identifying a client data area based on the source IP address, the client data area including the number of packets received; and
- incrementing the number of packets received.

The Office Action contends that Goldstone teaches all the limitations included in Applicants' claim 3, and uses paragraph 0038 in Goldstone as its basis for rejecting claim 3. However, upon closer inspection, Goldstone does not teach or suggest "identifying a client data area based on the source IP address, the client data area including the number of packets received... and incrementing the number of packets received" as claimed by Applicants. Rather, Goldstone's paragraph 0038 states that:

> "...when a response is sent from the server to the client, acknowledging the intention to connect, the attacking client merely ignores the response, resulting in a half-open connection... The server under these circumstances, not realizing that there is no intention to connect, assumes that the request is legitimate and reserves buffer space for the connection...[and] the server's bandwidth will still get congested since the attacking client will continue to send bogus requests to the server." (emphasis added)

As can be seen, the Office Action reference discusses a server's bandwidth becoming congested because the server accepts bogus packet requests from a malicious client, and never teaches or suggests "identifying a client data area based on a source IP address, the client data area including the number of packets received... and incrementing the number of packets received" as claimed by Applicants.

The Examiner mentioned that it is inherent that a client increments the number of packets when Goldstone's client sends packets. Applicants, however, are not claiming the client

incrementing the number of packets sent, but rather a receiving device, such as a server, incrementing the number of packets received. Applicants compare the number of packets received with one or more configuration settings in order to determine whether to perform an action, such as reject a client's packet (claim 1 limitations). The Office Action states that Gupta fails to teach the limitations in Applicants' claim 3, and indeed Gupta does not. Therefore, since neither Gupta nor Goldstone teach or suggest, in whole or in part, all the limitations included in Applicants' claim 3, claim 3 is allowable.

Claim 10 is an information handling system claim including the same limitations of claim 3 and, therefore, is allowable for the same reason as claim 3. Claim 16 is a computer program product claim including the same limitations of claim 3 and, therefore, is allowable for the same reason as claim 3.

Claims 7, 13, and 20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Gupta in view of Klaus (U.S. Patent No. 5,892,903, hereinafter "Klaus"). Applicants respectfully traverse these rejections.

Notwithstanding the fact that claim 7 is dependent upon amended claim 1 and therefore allowable for the same reasons as amended claim 1, claim 7 adds the limitations to amended claim 1 of:

- providing a test script, the test script including one or more attack simulations;
- processing the attack simulations included in the test script;

- determining whether to change one or more of the configuration settings based on the processing; and
- changing one or more of the configuration settings based on the determination.

The Office Action contends that Klaus teaches all the limitations included in Applicants' claim 7, and uses column 9, lines 1-41 in Klaus as its basis for rejecting claim 7. However, upon closer inspection, Klaus does not teach or suggest "*determining whether to change one or more of the configuration settings based on the processing, and changing one or more of the configuration settings based on the determination*" as claimed by Applicants. Rather, Klaus's reference states that:

> "...the system includes an IP spoofing attack generator 32, a source/destination address generator 34 and a service command generator 36. Source/destination address generator 34 identifies the internet and physical addresses of the computers on the network 12 to be tested. Source/destination address generator 34 verifies that each computer on network 12 is emulated in IP spoofing attacks on all of the other computers on network 12. In this manner, the inventive system exhaustibly tests all possible attack combinations on a network. Service command generator 36 generates commands for a service which may be coupled to a port which IP spoofing attack generator 32 is able to initiate a communications connection... The service command received from command message generator 36 and the source and destination addresses received from source/destination address generator 34 are used by IP spoofing attack generator 32 to provide data and header content for messages sent to transport layer 22 and network layer 24 of protocol stack 20 which are used to implement the IP spoofing attack and detection"

As can be seen, the Office Action reference discusses how Klaus tests a computer network for IP spoofing, but never teaches or suggests an action to take based on the results of the tests, let alone "*determining whether to change one or*

more of the configuration settings based on the processing, and changing one or more of the configuration settings based on the determination" as claimed by Applicants. The Office Action states that Gupta fails to teach the limitations in Applicants' claim 7, and indeed Gupta does not. Therefore, since neither Gupta nor Klaus teach or suggest, in whole or in part, all the limitations included in Applicants' claim 7, claim 7 is allowable.

Claim 13 is an information handling system claim including the same limitations of claim 7 and, therefore, is allowable for the same reason as claim 7. Claim 20 is a computer program product claim including the same limitations of claim 7 and, therefore, is allowable for the same reason as claim 7.

5. Claim Additions

Applicants have added claims 21 through 26 to the subject application in this amendment. Each of claims 21 through 26 are supported in the original specification and, therefore, do not add new subject matter.

Notwithstanding the fact that claims 21, 23, and 25 are dependent upon claims 1, 8, and 14, respectively, and therefore allowable for the same reasons as amended claims 1, 8, and 14, claims 21, 23, and 25 add "two-tiered" packet handling limitations to their respective independent claims of 1) determining that the number of packets exceeds a first limit and sending a notification, 2) receiving a subsequent packet that increments the number of packets, and 3) determining that the incremented number of packets exceeds a

second limit and rejecting the subsequent packet. Gupta, Goldstone, and Klaus do not teach or suggest, in whole or in part, determining that a number of packets exceeds a first limit and a second limit as claimed by Applicants and, therefore, claims 21, 23, and 25 are allowable over the art of record.

Notwithstanding the fact that claims 22, 24, and 26 are dependent upon claims 1, 8, and 14, respectively, and therefore allowable for the same reasons as amended claims 1, 8, and 14, claims 22, 24, and 26 add the limitations to their respective independent claims of 1) determining that the number of packets is higher than a historical usage, and 2) sending a notification in response to determining that the number of packets is higher than the historical usage. Gupta, Goldstone, and Klaus do not teach or suggest, in whole or in part, tracking a historical usage, let alone determining that the number of packets is higher than a historical usage as claimed by Applicants and, therefore, claims 22, 24, and 26 are allowable over the art of record.

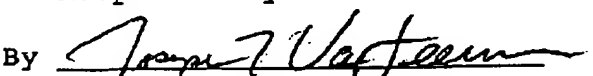
CONCLUSION

As a result of the foregoing, it is asserted by Applicants that the amended claims in the Application are in condition for allowance, and Applicants respectfully request an early allowance of such claims.

Applicants respectfully request that the Examiner contact the Applicants' attorney listed below if the Examiner believes

that such a discussion would be helpful in resolving any remaining questions or issues related to this Application.

Respectfully submitted,

By 

Joseph T. Van Leeuwen
Attorney for Applicants
Registration No. 44,383
Telephone: (512) 301-6738
Facsimile: (512) 301-6742

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:
Banerjee, et. al.

Serial No.: 09/870,610

Filed: May 31, 2001

Title: System and Method for Extending Server Security Through Monitored Load Management

§ **Group Art Unit: 2141**
§ **Confirmation No.: 1787**
§ **Examiner: Bayard, Djenane M**
§
§ **Attorney Docket No. AUS920010361US1**
§ **Intellectual Property Law Department**
§ **International Business**
§ **Machines Corporation**
§ **Intellectual Property Law Dept.**
§ **11400 Burnet Road**
§ **Austin, Texas 78758**

DECLARATION UNDER 37 C.F.R. § 1.131

Hon. Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Dwip N. Banerjee declares as follows:

1. I am an Applicant for the patent application entitled "System and Method for Extending Server Security Through Monitored Load Management," Serial No. 09/870,610, filed May 31, 2001, and an inventor of the subject matter described and claimed therein.

2. Prior to January 31, 2001, I conceived of, in the United States of America, the invention described and claimed in the subject application. I further showed diligence from the date of conception to the filing date of the subject application. Conception and diligence to filing is evidenced by the following:

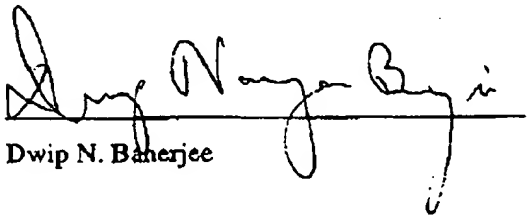
a. I submitted IBM Invention Disclosure Form No. AUS8-2001-0141, attached as Exhibit A hereto, which describes the invention described and claimed in the subject application.

b. Each of the dates deleted from Exhibit A is prior to January 31, 2001.

c. I worked diligently with a patent attorney in order to file the subject application on May 31, 2001.

3. I further declare that all statements made herein of my own knowledge and all statements made on information and belief are believed to be true; and further that these statements are made with the knowledge that willful and false statements and the like so made are punishable by fine or imprisonment or both under § 1001 of Title 18 of United States Code and that such willful and false statements may jeopardize the validity of the above-referenced application and any patent issuing therefrom.

FURTHER DECLARANT SAYETH NOT.



Dwip N. Banerjee

Date: 04/20/05

Attachment A

Disclosure AUS8-2001-0141

Prepared for and/or by an IBM Attorney - IBM Confidential

Created By: Vasu Vallabhaneni **Created On:** [redacted] 09:32:13 AM
Last Modified By: Vasu Vallabhaneni **Last Modified On:** [redacted] 09:15:28 AM

Required fields are marked with the asterisk (*) and must be filled in to complete the form.

***Title of disclosure (in English)**

Extending Server Security Through Monitored Load Management

Summary

Status	Under Evaluation
Processing Location	AUS
Functional Area	3P - SD-DEVELOPMENT AIX/6000; (H. ARMITAGE)
Attorney/Patent Professional	Volel Emile/Austin/IBM
IDT Team	Gerald McBrearty/Austin/IBM; Kenneth Banning/Austin/IBM; Johnny Shieh/Austin/IBM; Thomas Weaver/Austin/IBM; Kim Tran/Austin/IBM; Arthur Tysor/Austin/IBM; Deanna Brown/Austin/IBM; Alan MacKay/Austin/IBM; Dwip N Banerjee/Austin/IBM
Submitted Date	[redacted] 12:23:49 PM EST
Owning Division	SD
Incentive Program	
Lab	
Technology Code	
PVT Score	No PVT score has been calculated.To calculate a PVT score, press the 'Calculate' button.

Inventors with Lotus Notes IDs

Inventors: Vasu Vallabhaneni/Austin/IBM, Dwip N Banerjee/Austin/IBM, Vinit Jain/Austin/IBM

Inventor Name	Inventor Serial#	Div/Dept	Inventor Phone	Manager Name
Vallabhaneni, Vasu	3A8504	7T/D58S	678-2588	Haug, J.A. (Jessie)
Banerjee, Dwip N.	1A7337	7T/D58S	678-2747	Haug, J.A. (Jessie)
Jain, Vinit	2A1996	7T/D58S	678-9424	Haug, J.A. (Jessie)

> denotes primary contact

Inventors without Lotus Notes IDs

IDT Selection

Select Functional Area

IDT Team:	Attorney/Patent Professional:
Gerald McBrearty/Austin/IBM	Volel Emile/Austin/IBM

Kenneth Banning/Austin/IBM Johnny Shieh/Austin/IBM Thomas Weaver/Austin/IBM Kim Tran/Austin/IBM Arthur Tysor/Austin/IBM Deanna Brown/Austin/IBM Alan MacKay/Austin/IBM Dwip N Banerjee/Austin/IBM	

Response Due to IP&L : 02/24/2001

***Main Idea**

1. Describe your invention, stating the problem solved (if appropriate), and indicating the advantages of using the invention.
In the client server model servers which are listening on ports for clients can come under attack from malicious clients which could keep the server busy handling them. This can result in loss of server time and the worst case scenario of the server crashing due to excessive load.

2. How does the invention solve the problem or achieve an advantage,(a description of "the invention", including figures inline as appropriate)?
This problem can be solved by a kernel extension / deamon which will be monitoring the packets being received at the IP layer and maintain client usage statistics as per the example given below.

Source IP	Number_of_Packets Recd	Number_of_Packets Allowed	Time_Interval (in secs)	ServerPort	Action
9.3.149.49	200	500	2	UDP53	Block
202.4.4.4	500	300	2	UDP53	
Inf_adm					

Source IP :- IP address of the client.
Number_of_Packets Recd :- Number of packets received from client in the given Time_Interval.
Number_of_Packets Allowed :- Number of packets allowed to be received from the client in the given Time_Interval.
ServerPort :- Port number being monitored.
Action :- Action to be taken if the client is sending more number of packets in the given time interval than allowed. For example

- Block - Block the client i.e. set up a filter so that the packet from the client for given port doesn't reach the application (the packet gets dropped at IP layer.
- Inf_adm - Inform the system administrator.

Number_of_Packets Allowed, Time_Interval, ServerPort and Action are set by the system administrator in the configuration file.

The above solution can be further extended to do the following

1) Monitor the number of sockets opened for a given client to avoid DoS attacks.
2) Can be used for Accounting and Billing for Services.
3) Set customisable service management mechanisms on the server.

One of the advantages of our solution is that it can be used as a cheap solution to protect and regulate

access to systems / services outside a firewall and can also be used with firewalls to provide even stricter security.

3. If the same advantage or problem has been identified by others (inside/outside IBM), how have those others solved it and does your solution differ and why is it better?
We are not aware of similar solutions proposed by anyone else.

4. If the invention is implemented in a product or prototype, include technical details, purpose, disclosure details to others and the date of that implementation.
We are not aware of any implementation.

***Critical Questions (Questions 1-9 must be answered)**

***Question 1**
On what date was the invention workable? [redacted] **Please format the date as MM/DD/YYYY**
(Workable means i.e. when you know that your design will solve the problem)

***Question 2** ○ Yes ● No
Is there any planned or actual publication or disclosure of your invention to anyone outside IBM?

If yes, Enter the name of each publication or patent and the date published below.
Publication/Patent:
Date Published or Issued:

Are you aware of any publications, products or patents that relate to this invention? ○ Yes ● No

If yes, Enter the name of each publication or patent and the date published below.
Publication/Patent:
Date Published or Issued:

***Question 3** ○ Yes ● No
Has the subject matter of the invention or a product incorporating the invention been sold, used internally in manufacturing, announced for sale, or included in a proposal?

Is a sale, use in manufacturing, product announcement, or proposal planned? ○ Yes ● No

If Yes, identify the product if known and indicate the date or planned date of sale, announcements, or proposal and to whom the sale, announcement or proposal has been or will be made.
Product:
Version/Release:
Code Name:
Date:
To Whom:
If more than one, use cut and paste and append as necessary in the field provided.

***Question 4**
Was the subject matter of your invention or a product incorporating your invention used in public, e.g., outside IBM or in the presence of non-IBMers?

If yes, give a date. **Please format the date as MM/DD/YYYY** ○ Yes ● No

AUS8-2001-0141 Extending Server Security Through Monitored Load Management - continued

***Question 5**
Have you ever discussed your invention with others not employed at IBM?
○ Yes ● No

If yes, identify individuals and date discussed. Fill in the text area with the following information, the names of the individuals, the employer, date discussed, under CDA, and CDA #.

***Question 6**
Was the invention, in any way, started or developed under a government contract or project?
○ Yes ● No ○ Not sure

If Yes, enter the contract number

***Question 7**
Was the invention made in the course of any alliance, joint development or other contract activities?
○ Yes ● No ○ Not Sure

If **Yes**, enter the following **(In English)**:

Name of Alliance, Contractor or Joint Developer
Contract ID number
Relationship contact name
Relationship contact E-mail
Relationship contact phone

***Question 8**
Have you, or any of the other inventors, submitted this same invention disclosure or similar invention disclosure previously?
○ Yes ● No

If Yes, please provide disclosure number below:

***Question 9**
Are you, or any of the other inventors, aware of any related inventions disclosures submitted by anyone in IBM previously?
○ Yes ● No

If Yes, please provide the docket or disclosure number or any other identifying information below:

Question 10
What type of companies do you expect to compete with inventions of this type? *Check all that apply.*

- ☒ Manufacturers of enterprise servers
- ☒ Manufacturers of entry servers
- ☐ Manufacturers of workstations
- ☐ Manufacturers of PC's
- ☐ Non-computer manufacturers
- ☒ Developers of operating systems
- ☒ Developers of networking software
- ☒ Developers of application software
- ☒ Integrated solution providers
- ☐ Service providers
- ☐ Other (Please specify below)

Question 11
If the invention relates to a product or service that is outside the scope of your business unit, please recommend IBM business unit(s), IBM location(s) or individual(s) within IBM that you think would provide a good evaluation of your invention:

Patent Value Tool (Optional - this may be used by the inventor and attorney to assist with the evalua
(The Patent Value tool can be used by the inventor(s) to determine the potential licensing value of your invention.)
No PVT score has been calculated. To calculate a PVT score, press the 'Calculate' button.

Market
What is the anticipated annual market size (in dollars) that will be captured by your invention?

CLAIMS
Question 1 - How new is the technical field?

Question 2 - How central is the invention to the product(s) which might be expected to contain the invention?

Question 3 - What is the scope of the claim?

PORTFOLIO NEED
What are the portfolio needs in the area of your invention?

EXPLOITATION & ENFORCEMENT
Question 1 - How easily can the use of the Invention by a competitor be detected?

Question 2 - How easily can the use of the invention be avoided by a competitor?

BUSINESS VALUE
Question 1 - What percentage of the companies producing products in the field of this invention might use this invention?

Question 2 - What is the value of this patent to current or anticipated Alliance Activity between IBM and other companies?

Question 3 - What is the value of this patent to current or anticipated Technology Transfer Activity between IBM and other companies?

Question 4 - Does it result in prestige to IBM?

Post Disclosure Text & Drawings
Enter any additional information relating to this disclosure below:

(Form Revised 12/17/97)